

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 964 374 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
15.12.1999 Bulletin 1999/50

(51) Int Cl.⁶: **G07F 19/00**, **G07F 9/02**,
G06F 17/30

(21) Application number: **99303409.9**

(22) Date of filing: **30.04.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **27.05.1998 US 77337**
07.07.1998 US 91887 P
07.08.1998 US 95626 P
02.09.1998 US 98907 P
17.11.1998 US 193646

(71) Applicant: **DIEBOLD, INCORPORATED**
North Canton, OH 44720 (US)

(72) Inventors:
• **Drummond, Jay, Paul**
Massillon, Ohio 44646 (US)
• **Blackson, Dale**
Canton, Ohio 44718 (US)
• **Cichon Bob A.**
Massillon Ohio 44646 (US)
• **Covert, Mark, S.**
NW North canton, Ohio 44720 (US)

- **Moales, Mark, A.**
North Canton, Ohio 44720 (US)
- **Smith, Mark, D.**
NW, North Canton, Ohio 44720 (US)
- **Ess, Joseph, C.**
North Canton, Ohio 44720 (US)
- **Weis, David, W.**
Ashland, Ohio 44805 (US)
- **Richards, Bruce, G.**
North Canton, Ohio 44720 (US)
- **Church, James**
Kent, Ohio 44240 (US)

(74) Representative:
Purvis, William Michael Cameron et al
D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

Remarks:

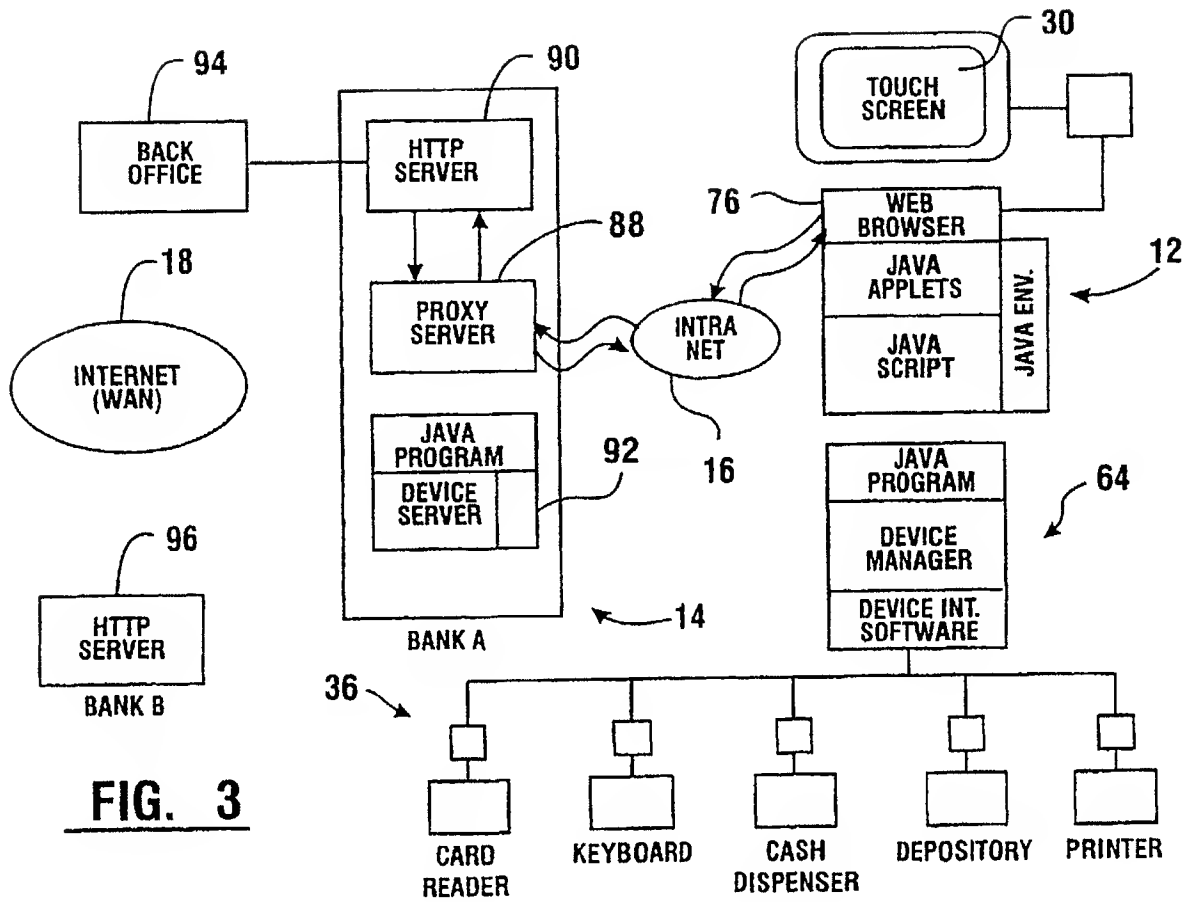
A request for correction of Fig. 25 has been filed pursuant to Rule 88 EPC. A decision on the request will be taken during the proceedings before the Examining Division (Guidelines for Examination in the EPO, A-V, 3.).

(54) **Transaction data object features including persistence, passing object and using object data for printing**

(57) An automated banking machine (12) is operative to conduct transactions in response to HTML documents and TCP/IP messages exchanged with a local computer system (14) through an intranet (16), as well as in response to messages exchanged with foreign servers (20, 22, 24, 26, 28,) in a wide area network (18). The banking machine includes a computer having an HTML document handling portion. The HTML document handling portion is operative to communicate through a proxy server, with a home HTTP server in the intranet or the foreign servers in the wide area network. The computer further includes a device application portion which interfaces with the HTML document handling portion and dispatches messages to operate devices in the automated banking machine. The devices include a

sheet dispenser mechanism which dispenses currency as well as other transaction devices. The device application portion communicates with a device interfacing software portion in the banking machine through a device server in the intranet. The device server maintains local control over the devices in the banking machine including the sheet dispenser. The banking machine operates to read indicia on the user's card corresponding to a system address. The computer is operative to connect the banking machine to the home or foreign server corresponding to the system address, which connected server operates the banking machine until the completion of transactions by the user.

EP 0 964 374 A2

**FIG. 3**

Description

[0001] This invention relates to automated banking machines.

[0002] Automated banking machines are well known. A common type of automated banking machine used by consumers is an automated teller machine ("ATM"). ATMs enable customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the making of deposits, the transfer of funds between accounts, the payment of bills and account balance inquiries. The type of banking transactions a customer can carry out are determined by capabilities of the particular banking machine and the programming of the institution operating the machine. Other types of automated banking machines may allow customers to charge against accounts or to transfer funds. Other types of automated banking machines may print or dispense items of value such as coupons, tickets, wagering slips, vouchers, checks, food stamps, money orders, scrip or travelers checks. For purposes of this disclosure an automated banking machine or automated transaction machine shall encompass any device which carries out transactions including transfers of value.

[0003] Currently ATMs are operated in proprietary communications networks. These networks interconnect ATMs operated by financial institutions and other entities. The interconnection of the networks often enables a user to use a banking machine operated by another institution if the foreign institution's banking machine is interconnected with the network that includes the user's institution. However when the customer operates the foreign institution's machine the customer must operate the machine using the customer interface that has been established by the foreign institution for its banking machines. In addition the user is limited to the transaction options provided by the foreign institution.

[0004] A customer may encounter difficulties when using a foreign institution's machine. Problems may occur because the user is not familiar with the type of machine operated by the foreign institution. Confusion may result because the customer does not know which buttons or other mechanisms to actuate to accomplish the desired transactions. The transaction flow for a customer at a foreign institution machine may be significantly different from machines operated by the user's home institution. This may be particularly a problem when the user is from another country and is not familiar with the type of banking machine or the language of the interface provided by the foreign institution. Likewise, the documents which are printed by printers in an automated banking machine are generally limited to a limited group of defined formats in a single language.

[0005] A foreign institution may also provide different types of transactions than the user is familiar with at their home institution. For example the user's home institu-

tion may enable the transfer of funds between accounts through their automated banking machines, to enable the user to maintain funds in higher interest bearing accounts until they are needed. If the foreign institution does not provide this capability, the user will be unable to do this when operating the foreign machine. The inability of a user at a foreign machine to conduct the transactions that they are accustomed to may present problems.

[0006] The networks that operate automated teller machines and other types of automated banking machines generally operate proprietary networks to which access is restricted. This is necessary to prevent fraud or tampering with the network or user's accounts. Proprietary networks are also generally used for the transmission of credit card messages and other financial transaction messages. Access to such credit card processing systems is also restricted primarily for purposes of maintaining security.

[0007] Communication over wide area networks enables messages to be communicated between distant locations. The best known wide area network is the Internet which can be used to provide communication between computers throughout the world. The Internet is not widely used for financial transaction messages because it is not a secure system. Messages intended for receipt at a particular computer address may be intercepted at other addresses without detection. Because the messages may be intercepted at locations that are distant in the world from the intended recipient, there is potential for fraud and corruption.

[0008] Companies are beginning to provide approaches for more secure transmission of messages on the internet. Encryption techniques are also being applied to Internet messages. However the openness of the Internet has limited its usefulness for purposes of financial messages, particularly financial messages associated with the operation of automated banking machines.

[0009] Messages in wide area networks may be communicated using the Transmission Control Protocol/Internet protocol ("TCP/IP"). U.S. Patent No. 5,706,422 shows an example of a system in which financial information stored in databases is accessed through a private wide area network using TCP/IP messages. The messages transmitted in such networks which use TCP/IP may include "documents" (also called "pages"). Such documents are produced in Hypertext Markup Language ("HTML") which is a reference to a type of programming language used to produce documents with commands or "tags" therein. The tags are codes which define features and/or operations of the document such as fonts, layout, imbedded graphics and hypertext links. HTML documents are processed or read through use of a computer program referred to as a "browser". The tags tell the browser how to process and control what is seen on a screen and/or is heard on speakers connected to the computer running the browser when the document

is processed. HTML documents may be transmitted over a network through the Hypertext Transfer Protocol ("HTTP"). The term "Hypertext" is a reference to the ability to embed links into the text of a document that allow communication to other documents which can be accessed in the network.

[0010] Thus there exists a need for an automated banking machine and system that can be used in a wide area network such as the Internet while providing a high level of security.

[0011] Various aspects of the invention are exemplified by the attached claims and by the list of sequentially numbered clauses 1 to 220 found at the end of the description.

[0012] It is therefore possible to provide:

an automated banking machine and system which provides a user with the familiar interface and transaction options of their home institution when operating foreign institution machines:

an automated banking machine which may provide more transaction options and types of promotional and printed materials to users:

an automated banking machine at which a user may conduct transactions:

an automated banking machine that may be operated through connection to a wide area network:

an automated banking machine that provides greater options for machine outputs:

an automated banking machine that communicates using HTML documents and TCP/IP messages:

an automated banking machine that enables the connection of the banking machine to a user's home institution through HTML documents and TCP/IP messages generated responsive to indicia on a card input by a user:

an automated banking machine and system that accomplishes transactions over a wide area network while maintaining a high level of security:

an automated banking machine and system that controls connection of the banking machine to foreign addresses through a proxy server;

an automated banking machine that limits the operation of devices in the machine through a local device server:

an automated banking machine and system that is operable through connection to the Internet:

an automated banking machine that may be used to provide a user with more types of messages including messages targeted to particular users:

an automated banking machine which is capable of providing users with a wider variety of printed documents:

an automated banking machine which provides additional options for identifying authorized users:

an automated banking machine that can be used in connection with existing transaction systems while providing enhanced functionality:

an automated banking machine which provides enhanced diagnostic and service capabilities:

an automated banking machine which performs transactions at a rapid pace:

improved systems in which automated banking machines are used: and/or

improved methods of operation for automated banking machines and systems.

[0013] According to one embodiment of the invention there is provided an automated banking machine that includes an output device such as a display screen, and an input device such as a touch screen or a keyboard. The banking machine further includes devices such as a dispenser mechanism for sheets of currency, a printer mechanism, a card reader/writer, a depository mechanism and other physical transaction function devices that are used by the machine to accomplish banking transactions.

[0014] The banking machine further includes a computer. The computer is in operative connection with the output devices and the input devices, as well as with the sheet dispenser mechanism, card reader and other physical transaction function devices in the banking machine. The computer includes software programs that are executable therein. The software programs include an HTML document handling portion. The HTML document handling portion operates to send and receive HTML documents and HTTP messages. The HTML document handling portion is preferably in connection with the output device to display screens including hypertext link indicators. The HTML document handling portion is also preferably in connection with the input device which enables user selection and the generation of response messages from the computer. The HTML document handling portion preferably operates in connection with a JAVA software environment and has the capability of executing instructions in JAVA script transmitted with HTML documents.

[0015] The software in the computer further prefera-

bly includes a device application portion. The device application portion includes software that is operative to control the sheet dispenser and other devices. In one embodiment of the invention the device application portion includes a plurality of JAVA applets for operating the devices in the machine.

[0016] The computer in the automated banking machine further includes a device interfacing software portion. The device interfacing software portion operates to receive messages from the device application portion and to cause the devices to operate through appropriate hardware interfaces. In one preferred form of the automated banking machine, the HTML document handling portion, device application portion and device interfacing software portion each reside on the same computer and communicate at different IP ports.

[0017] The automated banking machine in one configuration communicates using TCP/IP messages in an intranet which includes a plurality of such machines. The intranet is in turn connected to at least one computer which is operated by a home institution. The home institution is the entity that operates the banking machines.

[0018] The computer of the home institution preferably includes a home HTTP server, a proxy server and a device server. The proxy server communicates through the intranet with the HTML document handling portion of the software in each of the banking machines. The proxy server is also connectable to a wide area network, such as the Internet, to which foreign servers are connected. The device server is operative to pass messages between the device application portion and the device interfacing software portion of the banking machines. The device server may include monitor software which monitors and selectively limits the use and operation of the devices in the banking machine. This provides a level of security.

[0019] The automated banking machine and system is operative to place a user in connection with the institution where they have their accounts. This can be either the home institution that operates the banking machine where the user is present, or a foreign institution which is connected to the wide area network. To operate the banking machine a user provides inputs which correspond to an address, such as a URL address, through an address input device. The HTML document handling portion operates to connect the banking machine to the server corresponding to that address. This is preferably accomplished by the user having indicia representative of the address on a card that is read by a card reader in the banking machine, or other input device which identifies the user or an institution or entity with which the user has accounts.

[0020] The HTML document handling portion is responsive to the address on the card or other input data to connect through the proxy server to the user's institution. If the user's home institution address corresponds to the home server, the banking machine oper-

ates responsive to messages from the home server. If however the user's input address corresponds to an address of a foreign server, the proxy server is operative to communicate through the wide area network with the foreign server at the customer's home institution. If the customer causes the machine to connect a server operated by a foreign institution, the HTML documents sent from the foreign institution correspond to those normally provided by the foreign institution. As a result the customer is familiar with the interface produced by these documents and will be able to more readily operate the banking machine.

[0021] The foreign server or home server operate the banking machine by sending HTML documents that include instructions for operating the devices in the banking machine. The instructions are transmitted from the HTML document handling portion to the device application portion of the software, which operates the devices in response to the instructions. The instructions from the device application portion to the devices in the automated banking machine are passed through the device server of the home institution. This helps to maintain security. In addition, the proxy server includes screening software which limits the foreign servers which may connect to and operate the banking machine. This is referred to as a "fire wall."

[0022] Some embodiments of the present invention also provide enhanced user interfaces and for the printing of a wide variety of documents with the banking machine. Some embodiments enable achieving enhanced functionality while utilizing existing transaction networks and automated transaction machines.

BRIEF DESCRIPTION OF DRAWINGS

[0023] Figure 1 is a schematic view of a network configuration including an automated banking machine apparatus and system.

[0024] Figure 2 is a schematic view of one embodiment of an automated banking machine.

[0025] Figure 3 through 24 show schematic views of the automated banking machine, an intranet connecting the banking machine to a computer system of a home bank and a wide area network connecting the computer system of the home bank to a foreign bank.

[0026] Figures 3 through 18 schematically represent steps in a transaction carried out at the banking machine with the computer system of the home bank.

[0027] Figures 19 through 24 schematically represent steps in a transaction carried out at the banking machine with the computer system of the foreign bank.

[0028] Figure 25 is a schematic view of a network configuration including an alternative embodiment of an automated banking machine.

[0029] Figure 26 is a schematic view of frames in the HTML document handling portion of the alternative embodiment of the automated banking machine shown in Figure 25.

[0030] Figure 27 is a schematic view of a customer interface of an automated banking machine and function keys and keypad keys included in the interface.

[0031] Figures 28-30 schematically represent exemplary steps in converting function key and keypad key inputs to keyboard stream and mouse stream inputs.

[0032] Figure 31 schematically represents exemplary steps in printing documents with the automated banking machine.

[0033] Referring now to the drawings and particularly to Figure 1, there is shown therein a network configuration schematically indicated 10, which includes the automated banking machine apparatus and system of one preferred embodiment of the present invention. Network 10 includes a plurality of automated banking machines 12 which in this embodiment of the invention are ATMs. ATMs 12 are connected to a computer system of a home bank schematically indicated 14. Home bank computer system 14 is the computer system that is operated by the bank or other institution which has primary responsibility for the ATMs 12. Home bank computer system 14 is connected to the ATMs 12 through an intranet 16. Intranet 16 is preferably a local or proprietary network that provides communication between the computer system 14 and the banking machines 12 using messages in the transmission control protocol/internet protocol ("TCP/IP") format.

[0034] The messages that are communicated through the intranet 16 are preferably TCP/IP messages and hypertext mark up language ("HTML") documents. In one preferred embodiment of the invention the HTML documents sent through intranet 16 include embedded object oriented programming instructions, preferably in the JAVA® format which has been developed by Sun Microsystems. The messages sent through intranet 16 may be sent in an encrypted or unencrypted form depending on the nature of the system and the security needs of the home bank.

[0035] It should be understood that embodiments of the invention may process other forms of documents which include tags or instructions therein. For example a form of "extended" HTML has recently been proposed which may be used in embodiments of the invention. For purposes of this document all such forms of languages and variants which include documents, which documents include instructions therein shall be referred to as HTML documents. Likewise, while JAVA® is used in the described embodiment, other programming languages may be used. For example, Active-X™ developed by Microsoft Corporation or other languages may be used in other embodiments. Further it should be understood that the instructions included in documents may be operative to cause a computer to access other documents, records or files at other addresses to obtain a program to carry out an operation.

[0036] Home bank computer system 14 is also connectable as shown to a wide area network 18. In some embodiments of the invention the wide area network 18

is the Internet. In other embodiments of the invention, other wide area networks may be used. The wide area network preferably communicates messages in TCP/IP between numerous computer systems connected to the wide area network. These foreign computer systems are schematically represented by servers 20, 22, 24, 26 and 28. It should be understood that servers 20 through 28 may be operated by or connected to other financial institutions throughout the world. Servers 20 through 28 preferably operate by communicating HTML documents and other HTTP messages.

[0037] Figure 2 shows a schematic view of the ATM 12 used in connection with one preferred embodiment of the invention. ATM 12 includes a touch screen 30. Touch screen 30 includes a display screen which serves as an output device for communication with a user of the machine. Touch screen 30, because it is a touch screen, also serves as an input device for receiving input instructions from a user. Touch screen 30 is connected through an interface 32 to a computer 34 which is preferably housed within the machine. Alternative embodiments of the invention may include other output devices such as audio speakers.

[0038] Computer 34 is also in connection with a plurality of transaction function devices 36 which are included in ATM 12. Devices 36 include for example, a card reader/writer mechanism 38 and a keyboard 40. Devices 36 further include a sheet dispenser mechanism 42 which is operative to dispense sheets, which in some preferred forms of the invention are currency or bank notes. Devices 36 also include a depository 44 for accepting deposits into a secure location in the machine. A receipt printer 46 for providing transaction receipts to customers is also included among devices 36. A journal printer 48 is also included among the devices for keeping a hard copy record of transaction information. In other embodiments other or additional transaction function devices which carry out other transaction functions may be used. Other embodiments may include fewer transaction function devices. It should be further understood that while the described embodiment of the invention is an automated banking machine, the same principles may be employed in many types of transaction machines that do not necessarily carry out banking transactions.

[0039] Each of the devices is operatively connected to an internal control bus 50 within the banking machine 12. The control bus 50 outputs the internal messages to the particular devices. Each device has an appropriate hardware interface which enables the particular device to operate to carry out its respective function in response to the messages transmitted to it on control bus 50. Card reader/writer 38 has a hardware interface schematically shown as 52. Hardware interfaces 54, 56, 58, 60 and 62 are respectively operative to connect keyboard 40, sheet dispenser mechanism 42, depository mechanism 44, receipt printer mechanism 46 and journal printer mechanism 48 to the control bus 50.

[0040] Computer 34 has several software programs that are executable therein. In the preferred embodiment of the invention these software programs include a device interfacing software portion generally indicated 64. Device interfacing software portion 64 preferably includes a software device interface 66 that communicates electronic messages with the control bus 50. The device interface software portion 64 also preferably includes a device manager 68. The device manager is preferably operative to manage the various devices 36 and to control their various states so as to be assured that they properly operate in sequence. The device manager is also preferably operable to create device objects in the software so as to enable operation of the devices by at least one object oriented program 70. Device interfacing software portion 64 also includes the object oriented program portion 70, which in one preferred embodiment is an application written in the JAVA language. Program 70 works in conjunction with the device manager to receive object oriented JAVA messages which cause the devices to operate, and to transmit device operation messages indicative of a manner in which devices are operating and/or are receiving input data.

[0041] The device interfacing software portion 64 in the described embodiment operates on computer 34 and communicates through a physical TCP/IP connection 72 with the intranet 16. The physical connection may be analog dial-up, serial port, ISDN connection or other suitable connection. In the configuration of the system as shown, device interfacing software portion 64 communicates at the IP address of computer 34 and at an IP port or socket indicated 74 that is different from the other software applications. In other embodiments of the invention, device interfacing software portion 64 may operate in a different computer than the other software applications of the invention.

[0042] It should further be understood that although in the present embodiment of the invention the device interfacing portion 64 is software, in other embodiments of the invention all or portions of the instruction steps executed by software portion 64 may be resident in firmware or in other program media in connection with one or more computers, which are operative to communicate with devices 36. For purposes of this document all such forms of executable instructions shall be referred to as software.

[0043] Other software also operates in computer 34. This software includes HTML document handling software which includes a browser, schematically indicated 76. In the present embodiment of the invention the HTML document handling software includes a browser provided by Netscape®. However in other embodiments other HTML document handling and communicating software and browser software, such as Hot JAVA® by Sun Microsystems or Internet Explorer™ from Microsoft, may be used. Browser 76 communicates in computer 34 at an IP port indicated by 78.

[0044] Browser 76 is in operative connection with

JAVA environment software 80 which enables computer 34 to run JAVA language programs. JAVA language programs have the advantage that they operate the same on a variety of hardware platforms without modification. This "write once/run anywhere" capability makes the JAVA environment well-suited for the present embodiment of the invention. However other embodiments may use different types of software programs.

[0045] The JAVA environment software 80 enables computer 34 to execute instructions in JAVA script, schematically indicated 82. The instructions that are executed by the computer in JAVA script are preferably embedded JAVA script commands that are included in the HTML documents which are received through the browser 76. The browser 76 in connection with the JAVA environment software 80 which executes instructions in the embedded JAVA script 82, serve as an HTML document handling software portion for transmitting and receiving HTML documents and TCP/IP messages through the IP port indicated by 78.

[0046] Computer 34 also has executable software therein having a device application portion 84. The device application portion 84 contains executable instructions related to operation of the devices 36. In the preferred embodiment of the invention, the device application portion consists of a plurality of JAVA applets. In the described embodiment the applets are also preferably programs operable to control and keep track of the status of the devices with which they are associated. Certain applets are also preferably operable to configure the browser to communicate messages. Certain applets manage security and authenticate entities that use the ATM.

[0047] In the described embodiment of the invention, JAVA applets are associated with functions such as enabling the card reader mechanism, notifying the browser when a user's card data has been entered, operating the receipt printer mechanism, operating the journal printer mechanism, enabling the customer keyboard and receiving data input through the keyboard, operating the sheet dispenser mechanism, operating the depository, navigating to document addresses, timing device functions, verifying digital signatures, handling encryption of messages, controlling the mix of bills dispensed from multiple sheet dispenser mechanisms, calculating foreign exchange, and ending a transaction and instructing the browser to return to communication with the home server. Of course, in other embodiments, other applets may be used to control devices and use data to carry out various desired functions with the machine. The device application portion 84 communicates in the computer 34 at an IP port indicated 86.

[0048] In the described embodiment of the invention, the device application portion 84 of the software does not communicate its messages directly to the device interfacing software portion 64. As later explained, this provides heightened security. However it should be understood that embodiments of the invention may provide

for the device application portion 84 to directly communicate device operation messages to the device program 70. This may be done either internally using TCP/IP, by delivery of messages in a conventional manner through a queue established in the operating system of the computer that is associated with the software that interfaces with the devices, or by direct call to this software.

[0049] From the foregoing discussion it will also be appreciated that certain applets in the device application portion 84 may correspond to devices which are not present in all automated teller machines. For example an automated teller machine that operates only as a cash dispenser does not include a depository mechanism like depository 44. To accommodate the situation where a user requests a transaction that is not physically possible with the ATM 12, the device interfacing software portion 64 may be programmed to provide an appropriate response message to indicate that the function is not available.

[0050] Alternatively, the device interfacing software portion may include a function which checks for the presence or absence of each type of physical device within the ATM. Information indicative of the devices present in the ATM may be included as part of the messages generated by the ATM. For example, information indicative of the devices which are operative in the ATM may be included as a portion or several parts of the URL addresses to which messages are directed by the ATM. In this way, the URL in the server to which the ATM connects may be configured for providing only HTML documents which correspond to the types of transactions that the ATM is capable of performing. As a result the browser avoids displaying documents which include references to transaction types that the machine is not capable of performing. Thus for example, a machine may avoid producing a display in response to a document which includes a reference to a deposit transaction if the machine does not include a depository.

[0051] Alternatively the machine may include in memory, data representative of the functional devices included in the machine. This may include for example data representative of a plurality of devices in the machine and the configurations of such devices, or alternatively, a designator such as a machine number sufficient to identify the capabilities of the machine. The device data indicative of the functional devices in the machine is communicated to a server and the server is operative to deliver the appropriate HTML documents for the devices present in the machine. This may be done based on the data corresponding to the device data from the machine or may be resolved from a memory which holds data representative of the functional devices in a machine associated with a particular designator. Documents selectively delivered by the server to the browser of the machine will include the appropriate references to the functional devices present in the machine. These documents may be static documents or may be generated at

run time from subdocuments or otherwise, to provide the appropriate outputs and instructions to the output devices of the transaction machine.

[0052] Figure 3 shows the ATM 12 in communication through the intranet 16 with the home bank computer system 14. Computer system 14 includes a proxy server 88. System 14 further includes a home HTTP server 90. Computer system 14 further includes a device server 92. The proxy server, home HTTP server and device server may be included in a single computer as shown, or in other embodiments may be separate computers. Additional servers may be operative in other embodiments.

[0053] The home HTTP server 90 is preferably in communication with a data store and is in electronic communication with a back office computer system, schematically indicated 94. Back office computer system 94 is operative to keep track of debiting or crediting customers' accounts when they conduct transactions at the automated banking machines. In addition back office 94 is also preferably operative to track transactions for purposes of accomplishing settlements with other institutions who are participants in the system and whose customers conduct transactions at the ATMs 12.

[0054] As later explained, proxy server 88 is also operative in the described embodiment to communicate through the wide area network 18 with foreign servers such as foreign server 96. Foreign server 96 is an example of a server operated by an institution or entity other than the institution which operates computer system 14. It should be understood that while foreign server 96 is indicated as operated by a "foreign" institution, this is not necessarily indicative that the institution is located in another country from the institution that operates computer system 14. However, it is possible that foreign server 96 could be located in such a foreign country, including a country in which the language spoken is different from that generally used in the country where ATM 12 is located.

[0055] The conduct of transactions using the ATM 12 is now explained with reference to Figures 3-24. It should be understood that the following described transaction flows are merely examples of the operation of the apparatus and system, and the apparatus and system may be configured and operated in numerous ways to carry out transactions.

[0056] At the start of an exemplary transaction, as schematically represented in Figure 3, the browser 76 communicates through the intranet 16 with the proxy server 88. The communication is established preferably in a manner so that HTML documents intended to attract customers to the ATM 12 are displayed on the touch screen 30. This is referred to as the "attract mode." These HTML documents which are processed in the browser to produce the outputs in the form of screens on the touch screen 30 (and/or outputs through other output devices included in the machine) may originate from home HTTP server 90 which is operative to deliver

the HTML documents to the proxy server. The home HTTP server sends the messages addressed to the IP port associated with browser 76, so as to cause their display at the proper ATM machine. It should be understood that while in this example, home server 90 is described as communicating with the ATMs through the proxy server 88, the server 90 may in other systems encompassed by the invention communicate directly with the ATMs.

[0057] A fundamental advantage of the system is that home HTTP server 90 may deliver documents selectively to the ATMs 12 connected to the intranet 16. These documents may include messages or material tailored to the particular location in which an ATM 12 is located. Examples of particularly tailored screens may include bilingual messages in certain neighborhoods or information concerning currency exchange at various ports of entry. The material or messages could include advertising for various products or services or other material targeted to particular machine locations. The JAVA applets and JAVA script are loaded from a central location providing selective software distribution in the ATMs which may also be used to tailor the ATM to its environment by causing it to access documents which include material intended to be useful in that location, and which is not provided in documents delivered to at least some other machines in the system.

[0058] Systems of embodiment of the invention may be configured to have selected machines access HTML documents at different addresses, so that the particular documents accessed include the material targeted to users of the particular machine. Alternatively, a machine may communicate machine data indicative of its identity and/or location to a server. From the machine data, and data stored in a data store in connection with the server, the server operates to deliver the documents including the targeted material. This may be accomplished by assembling subdocuments, or otherwise, to generate the documents that will be delivered to the browser of the particular machine. In addition it should be understood that while in the embodiment shown the HTML documents are accessed through a server of an institution associated with the machine, the documents used for the attract mode may be accessed from other servers operated by other entities.

[0059] The touch screen 30 in this exemplary transaction sequence displays a screen which includes an icon which indicates in one or more languages that to commence a transaction a user should touch the screen. If a user touches the screen in the area of the icon an input signal is generated. The input signal or HTTP message is transmitted through the browser 76 to the home address of the home HTTP server 90 to which the ATM 12 is currently in communication. The message generated back to the home HTTP server is represented by the arrows directed from the browser 76 to the intranet 16, from the intranet 16 to the proxy server 88, and from the proxy server to the HTTP server 90 in Figure 3.

[0060] In response to the home HTTP server 90 receiving the message indicating that a customer has touched the icon on the screen, the home server is operative responsive to the address accessed to send a message through the proxy server 88 (or in other embodiments directly) to the browser 76. This message preferably includes an HTML document which when processed through the browser produces a screen instructing the customer to insert their card into the card reader mechanism 38. The HTML document flow which is represented graphically in Figure 4, preferably also includes embedded JAVA script or other instructions which operate in the JAVA environment to communicate a message to the JAVA applet responsible for enabling the card reader in the device application portion 84. In one preferred embodiment the instructions provide a pointer or tag to the applet which executes responsive to receipt of the document instructions. Of course in other embodiments other software and approaches may be used.

[0061] As shown in Figure 5, in response to the embedded JAVA script activating the JAVA applet associated with the enable card reader function, the JAVA applet in the device application portion 84 communicates with the device server 92. The device server 92 includes a device server program 98 which in the preferred embodiment is a JAVA program that enables communication with the JAVA applets and the device server application 100. The device server 92 further preferably includes a monitor software application 102 which is operative to monitor device operation instructions. The monitor software minimizes the risk of fraud or abuse in a manner later explained.

[0062] Returning to the sample transaction, in response to receiving the enable card reader message from the device application portion 84, the device server 92 is operative to generate a message through the intranet 16 to the device interfacing software portion 64 of the ATM 12. This message which comprises an HTTP record including instructions for operating the card reader, is directed to the IP port indicated 74 which is where the device interfacing software portion 64 communicates. In response to receiving this message, the software portion 64 is operative to send a message or messages on the control bus 50 which enables card reader mechanism 34.

[0063] Continuing with the transaction as shown in Figure 6, the input of the card by the customer to the card reader 34 is operative to cause the card data to be read and the device interfacing program portion 64 to send a message to the device server 92 indicating the card data has been read. This message is transmitted by the device server through the intranet 16 to the device application portion 84. The device application portion then sends a message to the device server requesting the card data. The device server 92 transmits a message with instructions to deliver the card data from the device interfacing software portion 64 which responds

with a message sending the card data through the intranet to the device server. The device server, if there is no basis for stopping the transaction, transmits an HTTP record including card data back through the intranet 16 to the device application portion 84.

[0064] In one preferred embodiment of the invention, the card input by a user or customer includes indicia which corresponds to an address associated with the user in the network. In such an embodiment the indicia corresponds to a uniform resource locator ("URL") address which provides information on the computer where the user information resides, as well as a directory or subdirectory which includes the user information and the name of the document or resource that includes the user information. The URL address may be encoded on a customer's card. The address may be encoded on track 3 of a magnetic stripe, in other locations within the magnetic stripe data or through encoding other readable indicia on the card. Alternatively, if the customer's card is a "smart" card which includes semiconductor storage thereon, the URL address associated with the customer may be included as part of the stored data on the integrated circuit chip on the customer's card. Alternatively, a URL could be derived from other data on the card by accessing a data base in which address data is correlated with other data read from the card. The data necessary to derive the address for accessing documents associated with a customer could also be derived from inputs to input devices other than or in addition to card data, including for example biometric data which is input by a customer through a biometric reading device. Such biometric data may include for example, data corresponding to one or more fingerprints, data from the user's appearance or combinations thereof.

[0065] For example and without limitation, data input by a customer such as through a card input to a card reader may correspond to an address for accessing an HTTP record, which may be a file or document which includes information which can be used for verifying the identity of a user. This record could include data corresponding to a PIN number. The information may include biometric data corresponding to the authorized user of the card. The browser may access the record and use the contents of the record such as data and/or instructions to verify that the indicia corresponding to biometric data in the record corresponds to the biometric data of the user entering the card. Alternatively, input data representative of appearance, voice, other features (or combinations thereof) or other input data, may be used to generate one or more addresses which correspond to a user, and the content of the record at the accessed address used to verify that the user at the machine corresponds to the user associated with the record. Numerous approaches within the scope of the invention may be used. The information in the record corresponding to a user may likewise be used to authorize certain functional devices on the machine to operate for the user while other devices may not. For example, a user who

is overdrawn may have information in the record accessed that prevents them from actuating the cash dispenser, while users who are not overdrawn may include information which enables such operation. Alternatively, the absence of information in a corresponding record may enable operation, while the inclusion of information selectively limits the operation of devices.

[0066] Returning to the exemplary transaction, the delivery of the card data from a successfully read card is delivered responsive to the programming of the device application portion 84 to a JAVA applet associated with notifying that the card data has been entered. In response, the JAVA applet operates to generate JAVA script which configures the browser with the URL address corresponding to the data read from the card. The JAVA applet is also preferably operative to open a record schematically indicated 104 concerning the transaction, which includes the user's URL address, the time and other card data. This record in a preferred embodiment may be stored in memory as data in an object in software. The object is preferably used to accumulate data as the transaction proceeds. The data stored in the transaction data object preferably includes data input through input devices by the user as well as data representative of operations carried out by transaction function devices.

[0067] The record or transaction data object provides persistence through what may be several different transaction steps executed by the customer. The ability to use and share the data in a number of different operations avoids the need to derive it or obtain it from a customer more than once in the course of a user session involving a number of transaction steps. The use of a transaction data object enables applets to run largely independently, obtaining needed data from the transaction object. The approach also enables the record or data object to be used to produce an appropriate record at the end of the transaction session. This record may be stored, collected into a batch or delivered to selected addresses in a local or wide area network.

[0068] As schematically shown in Figure 7, in response to the browser 76 receiving the URL address data, the browser is operative to transmit a message through the intranet 16 to the proxy server 88. For purposes of this example, the URL address associated with the card data is that of a customer associated with the home bank which operates system 14. As a result, the customer's URL address will cause the message to be directed from the proxy server 88 to the home HTTP server 90 and to access the corresponding document at the address therein. Alternatively, in other systems the connection may be made directly with server 90 without the intervening proxy server 88. As previously discussed, the URL address may also include data representative of the devices which are operative in the ATM.

[0069] In response to receiving the message, home HTTP server 90 finds the data corresponding to the customer's URL address data in its associated memory and

delivers to the browser at its IP port with an HTML document. This HTML document may include a screen acknowledging the particular customer by name as well as with the name of the banking institution or other entity which operates the home bank computer system 14.

[0070] In addition, the HTML document preferably includes embedded JAVA script which has a digital signature or a means to obtain a digital signature associated with the home HTTP server 90. The script instruction included in the document in certain embodiments causes the device application portion to access an HTTP address on a server, which in the described embodiment is server 90. The HTTP address corresponds to an HTTP record which includes at least one instruction and preferably includes a program such as a JAVA applet or Active-X file. The instruction is used to operate the appropriate transaction function device. The HTTP record preferably includes data representative of a signature, such as a digital signature. This digital signature is received responsive to the JAVA script 82 and processed in the device application portion 84. A JAVA applet processes the digital signature to authenticate it and if it is an acceptable signature authorizes operation of the banking machine. In certain embodiments the applet may compare the signature to signature data stored in memory for a predetermined relationship, such as a match.

[0071] After the applet verifies that HTTP server 90 or other accessed HTTP record has sent a proper digital signature, the transaction will be allowed to continue. If for some reason a proper digital signature has not been sent, the JAVA applet will stop the transaction and return banking machine 12 back to the condition prior to the start of the transaction by connecting the ATM to the address associated with the attract mode in home server 90. The use of signed instructions may be used to assure that the various transaction function devices are only operated in response to appropriate messages. The use of signed instructions may be particularly appropriate for instructions that run the sheet dispenser or otherwise provide value to the user of the machine.

[0072] In the example it will be assumed that the digital signature received is a proper signature, in which case a message is returned from the browser 76 to home server 90 indicating that the transaction may proceed. As shown in Figure 8, in this exemplary transaction the HTTP home server 90 then operates to send an HTML document to the browser 76 which includes instructions which when processed produce a page or screen which instructs the customer to enter their personal identification number or PIN. This HTML document preferably includes embedded JAVA instructions which operate to cause the device application portion 84 enable the keyboard 40 of the ATM so the machine may receive the PIN number. Such a message is schematically shown in Figure 8 with the JAVA script 82 signaling the JAVA applet responsible for the keyboard that it has been requested to enable the keyboard. In re-

sponse the JAVA applet in the device application portion 84 sends a message through the intranet 16 to the device server 92. The device server 92 sends a message back through the intranet to the device interfacing software portion 64 in the ATM. The instructions in this message causes the device software to enable keyboard 40. The JAVA applet responsible for enabling the keyboard is also preferably operative to update the transaction record 104 to indicate that the PIN was requested.

[0073] As shown in Figure 9, the PIN entered through the keyboard 40 is transmitted in a message from the device interfacing software portion 64 to the device server 92. The device server 92 returns a message to the responsible JAVA applet in the device application portion. The JAVA applet then operates to send a message back through the HTML document handling portion and the browser 76 to the HTTP address of home server 90. This message includes data representative of the PIN input by the customer. In some embodiments it is not desirable to display the customer's PIN on the screen. In such embodiments the keyboard applet may be operative to display a default character on the screen such as a "*" symbol or other symbol in lieu of the PIN digits. Further as later discussed it may be desirable to avoid transmission of PIN or other data through the browser, in which case PIN data may be handled as a separate HTTP message or in other manner to reduce the risk of disclosure.

[0074] The software operating in connection with HTTP server 90 is then operative to either verify the PIN itself or to verify the customer's PIN number and account number by sending it to the back office 94 and waiting for a response. Alternatively, customer PIN verification may be carried out in the ATM through an appropriate applet. This can be done in situations where data on a customer's card, such as an account number, can be correlated to the customer's PIN number through an algorithm. The embedded JAVA script in the HTML messages may include or point to an address to obtain the data and/or instructions which the applet uses to perform this verification function, including certain encryption key data. This may include user information in the HTML document or other record data that was accessed in response to the user's card data. As shown schematically in Figure 9, the transaction data object 104 is also appropriately updated by the applet to indicate the entry of the customer's PIN.

[0075] In alternative embodiments the machine may include a biometric reader device or other input device to accept data from a user. The user may input data through such a device which may be used in lieu of, or in addition to, PIN data to verify that the user is an authorized user. This may be done for example by comparing the user data input to information corresponding to the authorized user of the card included in a record or a document which has an HTTP address and is accessed by a browser or by an HTTP client application through an HTTP server in response to card data. Alter-

natively input data may be used to generate addresses for documents or records which are accessed by the browser or client, and which records or documents contain information that is used to verify the user's identity. For example, data concerning users may be stored in a data store in connection with an HTTP server, which delivers data from a record responsive to the user data, which is used to verify the user's identity.

[0076] It should be noted that the page or screen which requests the customer to enter their PIN is shown generated from the home HTTP server 90. This is preferably a screen that is associated with the particular customer's URL address. This will be the interface of the customer's home bank and will be familiar to the customer. Alternatively, the customer address may access what may be essentially the customer's personal "home page" with the institution that operates computer system 14. As such, it is not only something the user is familiar with, but is ideally tailored to the user's particular transaction needs.

[0077] Alternatively, the document(s) or record(s) which contain the customer data may be used to generate the addresses for other documents. The information may also be used to generate a document for the particular customer in the particular circumstances. This approach may be useful to reduce the effort associated with developing in advance a personal visual page or document for each customer.

[0078] Approaches for accomplishing this may involve including various types or categories of user information in the document(s) or record(s) that pertain to a particular customer. This may include information such as gender, related persons, account types, permitted transactions, customer preferences, customer interests, account balances, previous offers declined or accepted and other information. This customer information can be used by an appropriate applet among applets 86 to address and/or develop an appropriate document for the browser to access based on the customer "profile". In addition, the profile applet may take into consideration the transaction devices present in the particular machine, information on which is stored in a data store in the machine or elsewhere in the system, as well as other factors such as the day of the week and time of day based on a system clock. In this way the machine determines the appropriate document to access or generate for the particular customer under the particular circumstances.

[0079] The logic used in the profile applet may act to cause documents to be built or accessed for the customer which includes transaction options based on the customer information, information about the terminal and other factors. The profile applet may operate to offer transaction options or information selectively based on the customer information. For example, the operator of the machine may offer incentives, premiums, additional transaction options or advertising information selectively to customers. Certain types of customers of the insti-

tution operating the machine may receive screen outputs with options that encourage them to do more business or different types of business with the institution. Likewise, customers that are identified as customers of foreign institutions may be provided with incentives to do business with the institution operating the machine.

[0080] The profile applet may operate to cause the computer to access other documents in other servers, such as stock market data, and selectively provide it to customers. It should be understood that the profile applet may operate to determine an address or generate documents to produce initial display screens of a transaction sequence. The profile applet may also operate to provide information or access or produce documents to generate visual outputs to the customer at other points in a transaction or between transactions. This may further be used in systems in which the operator of the machine is able to sell paid advertising to third parties and then access the HTTP records such as HTML files for those third parties' products or services. Such accessing may be done based on a periodic or other basis, but may be done effectively by selecting the HTTP record to access in response to the profile of the particular customer.

[0081] The continuation of the transaction flow for this exemplary transaction by a customer of the institution that operates computer network 14, is schematically shown in Figure 10. The home HTTP server 90 is operative in response to the customer inputting the correct PIN to send HTML documents to the HTML document handling portion of the software in the computer which operates the ATM. These messages may include information used to generate screens which prompt the customer to select a transaction. For purposes of this example, it will be assumed that the customer inputs at the touch screen 30 a selection which corresponds to the dispense of cash, which is a common transaction at an automated banking machine.

[0082] The selection of the customer through the input device of the touch screen is communicated back through the HTML document handling portion which communicates an HTTP message to the home HTTP server 90. Server 90 then responds by sending another HTML document to the banking machine which prompts the customer to select an amount. Again the customer may input a selection on the touch screen which indicates the amount of cash requested by the customer. This HTTP message passes through the HTML document handling portion and the browser 76 to the home server 90.

[0083] In response to the receipt of amount data from the customer, the home server 90 is preferably operative to communicate electronically with the back office 94 to verify that the customer has the amount requested in their account. This is preferably accomplished through a Common Gateway Interface (CGI) 106 which is in operative connection with the home server 90. For purposes of this transaction it will be assumed that the back

office 94 indicates that the money is available in the customer's account and sends a message through the CGI 106 to the home server 90 indicating that it may proceed.

[0084] As schematically represented in Figure 11, the home server 90 then operates to send a document back to the HTML document handling portion in the ATM software. This message preferably will cause information to be displayed on the screen which advises the customer that the transaction is being processed. In addition the HTML document returned preferably includes JAVA script which include embedded instructions which are executed and communicated to a JAVA applet associated with the operation of the sheet dispensing mechanism 42.

[0085] The document returned from the home server 90 may include advertising or other information instead of or in addition to the customer message. The document returned may also include an instruction which causes the machine to access or generate another document. These instructions may invoke methods in the profile applet which depend on the properties associated with the customer, the machine, the current time and/or other circumstances. This enables accessing documents that provide promotional messages such as advertising or other information to the customer while the customer is waiting for the machine to operate. It should be understood that these documents may be accessed anywhere, including from the Internet. This makes it possible to selectively present a wide range of materials to customers. It also enables operators of ATMs and other transaction machines to present advertising to customers, on a broad basis, or targeted to categories of customers or even targeted to individual customers on a segment of one basis. This could be advertising of the machine operator such as a bank, or advertising pertaining to virtually any type of goods or services. The advertising may also be selectively presented based on the particular transaction device being operated, the amount of funds involved or other parameters. The HTML documents also enable the presentation of video and sound to the customer which may enhance the effectiveness of promotions.

[0086] The message to the JAVA applet in the device application portion 84 of the software to initiate operation of the sheet dispenser results in generation of a message to the device server 92. The message to the device server 92 to dispense cash is preferably analyzed by the monitor software 102 to check to see if the message is appropriate. For example the monitor software 102 is preferably operative to assure that the amount of cash being requested does not exceed a preset amount. It can also optionally check to verify that the amount provided to this customer within a prior period has not exceeded an amount. This may be done by the device server sending a message to the back office which includes the card data it has previously received from this customer. This message may pass through server 90 and its associated CGI, or other connection.

Assuming that the dispense instruction is not prevented by a message from the back office or the monitor software, the device server 92 is operative to send a dispense message to the device interfacing software portion 64 in the ATM. The software portion 64 is thereafter operative responsive to the message to operate the sheet dispensing mechanism 42 to dispense the amount of cash requested by the customer.

[0087] The monitor software 102 preferably performs additional functions in the device server. For example, government regulations or good business practice may require limiting the size and amounts of deposits which may be made into an ATM. This may be advisable to prevent "money laundering" or other suspicious activities. The monitor software preferably operates to limit the amount of any single deposit to below a set limit. It further operates by communicating with the home bank back office system 94 to prevent a series of deposits within a preset time from exceeding a certain limit. The monitor software may also work in connection with the proxy server to limit certain transactions that may be carried on at the banking machine responsive to instructions from foreign servers as later discussed.

[0088] It should be noted that in a preferred embodiment of the invention the JAVA applet which is operative to send the message which causes cash to be dispensed, works in connection with another applet which controls the mix of bills dispensed to a customer. Many automated teller machines have the ability to dispense two or more denominations of currency bills. It is desirable to control the mix of bills dispensed to a customer to suit that which is available in the machine and to avoid running out of one denomination of bills before the other. The bill mix applet is preferably operable to control the bill mix in accordance with the desires of the institution operating the ATM machine as well as is in accordance with the ATM machine's capabilities. Alternatively, a JAVA applet for controlling bill mix may reside in device program 70 in device interfacing software portion 64.

[0089] As will be appreciated by those skilled in the art, the particular JAVA applets and/or configuration data in the machine may be selectively loaded from the home server 90 at machine start up or at other times. Because the applets and configuration data may be selectively delivered to particular machines, the machines may be tailored specifically to the particular ATMs currency dispensing and other capabilities. For example, the ATM may be configured so that certain applets or groups of applets must be present to enable the machine to operate. One approach to loading such data or programs is to provide address values in the terminal software to indicate where the needed instructions to acquire the applets or data may be obtained. If the applets or groups of applets are not already present in memory of the ATM terminal at start up, the software is operative to access the system addresses for the documents which contain the required records or instructions which will cause the machine to load the required records. The

browser may be used to access the addresses and the software loads data corresponding to the instructions from the accessed documents into a memory in the ATM terminal so that the terminal has the required applets and data. Such document addresses may be accessible through the home server 90. Alternatively the addresses may be on a separate development server connected to the intranet 16. In this way each transaction machine is able to load the applets and data which include the operative code it needs to operate the transaction devices in the machine. Alternatively, the documents may be provided through a development server or other server that is accessible to the machine through a wide area network. The documents may be provided on the development server to provide the machine with instructions on how to acquire the operating code to carry out a wide variety of functions. The instructions may direct the machine to acquire the necessary data and code from addresses accessible through HTTP servers by an HTTP client in the machine. The data and code can be acquired responsive to instructions in one or several documents. The machine may also require that the applets loaded in this manner be signed applets including digital signatures or other authenticating features to achieve operation of certain devices in the machines.

[0090] Alternatively, embodiments of the invention may acquire the necessary applets and data from a remote data store. The data store preferably includes the data and/or programs that enable the machine to operate as desired or have instructions on where the machine may acquire the necessary instructions and data for operation. The data may be accessible from a database server. The transaction machine addresses a query to the database server. The query includes or is accompanied by indicia from the machine which identifies the machine. This may be the particular machine such as a machine number, and/or may include indicia representative of the type or functional device capabilities of the machine.

[0091] The data store preferably includes records which have the data or programs that are to be transmitted to the machine. In response to the query to the server, the server retrieves records from the data store and responsive thereto delivers one or more messages to the HTTP client in the transaction machine. This message(s) includes the configuration data or applets to enable the machine to operate in the manner desired or may include instructions which indicate how the machine is to acquire such programs from servers connected in the system.

[0092] In the example shown the configuration server and data store may operate on the same computer as home bank server 90. In other embodiments the database server may reside elsewhere in the networks to which the machine is connected.

[0093] An advantage of the machines and systems which employ such features is the flexibility to change the operation and customer interface of the machine to

respond to changing conditions. This may include a change in a transaction function device. Conditions may change so that certain transactions are limited or are not available. For example, a machine may normally accept deposits but its depository is full. In that situation the machine may change the documents it accesses to present messages to users through its output devices so that the deposit option is no longer offered. This can be accomplished by the applets and data loaded into the machine initially, which provide for instructions when such event is sensed. Alternatively, the machine programming may be modified by loading new applets and/or data from an HTTP server responsive to its then current status. This may be done responsive to a query to a database server which includes or is accompanied by data representative of the changed conditions or capabilities of the machine. In response the server delivers the applet(s), data and/or instructions which will operate the machine in the modified mode.

[0094] This approach eliminates the situation with conventional transaction machines where the static interface presentation on output devices offers a transaction option to a customer. Sometimes, after the customer has made the selection an indication is given that the selected transactions option is not available. The approach described herein may be used with numerous transaction options and variations of transactions. The transaction options can be readily changed from the database server on a machine by machine basis or even a customer by customer basis as previously discussed, based on the desires of the entity operating the transaction machine.

[0095] The discussion of the exemplary transaction will now be continued. In response to the cash dispenser 42 dispensing the requested amount of cash, device interfacing software program 64 preferably operates to send a dispense operation message confirming the dispense back to the JAVA applet responsible for the dispense in the device application program 84. As represented in Figure 12, the particular applet is operative to update the transaction record 104 to indicate the dispense of currency to the customer in the particular amount. The embedded JAVA script instructions which were operative to cause the dispense of currency to the customer, also preferably include instructions to send a confirming message back to the home server 90 that the dispense is complete. The receipt of the dispense operation message indicating the cash was dispensed causes the JAVA applet to configure the HTML document handling portion to send a device response message back to the home server. The home server then is preferably operated in accordance with its programming to indicate to the back office 94 that the customer received the amount of funds dispensed. This amount is deducted from the customer's account in the records maintained by the back office system.

[0096] Generally during a transaction it is common to ask the customer if they wish to have a receipt for the

transaction. This may be done at various times during the transaction flow. In the present example, after the cash has been dispensed the customer operating the machine is sent such a message as reflected in Figure 13. The home server 90 is operative to send an HTML document which includes a screen asking the customer if they would like a receipt. This message is displayed as part of a page on the touch screen 30 responsive to receipt of the message through the browser 76. Alternatively the document may be generated by the machine. In response to the customer indicating that they do or do not want a receipt, a message is returned to the home server. Again it should be understood that the screens displayed to the customer are preferably those that the customer is accustomed to from his or her home institution, and may be a part of his or her unique home page.

[0097] Assuming that the customer wishes to receive a transaction receipt, the home server 90 operates as shown in Figure 14 to send a document back to the ATM with embedded JAVA script indicating that a transaction receipt is to be printed. These instructions in JAVA script are communicated to the device application portion 84 which sends a TCP/IP message through the intranet to the device server 92. The device server 92 in turn communicates a message with instructions to the device interfacing software portion 64 in the ATM. In response to receiving the message, software portion 64 is operative to cause the printer 46 to print the customer's transaction receipt. The JAVA applet responsible for enabling the printer is also preferably operative to update the transaction data object or record 104. As later discussed, the applet which controls the printing of the receipt may obtain the data used in printing the receipt from the transaction data object.

[0098] It should be understood that even if the customer does not wish to have a receipt it is desirable to print a record of the transaction in hard copy through the journal printer 48. This may be accomplished in response to imbedded instructions which are part of the same document from the home server 90 which causes the transaction receipt for the customer to be printed, or may be part of a separate document which indicates that the customer has declined the option to receive a transaction receipt. Alternatively, the journal printer may be actuated responsive to other applets such as the applet which causes the dispense of cash, or in another manner chosen by the operator of the ATM. As will be appreciated from the foregoing description the operation of the present embodiment of the ATM is inherently flexible and programmable to meet the needs of the system operator.

[0099] As shown in Figure 15 upon completion of the printing of the transaction receipt, the software portion 64 is preferably operative to send a device operation message to the device server 92 which is indicative that the requested device function was carried out successfully. The device server 92 is operative to send a corre-

sponding device operation message to the device application portion 84, and in the preferred embodiment to the particular JAVA applet responsible for the printing of the receipt. The JAVA applet in turn configures the HTML document handling portion to generate a message back to the home server in the form of a device response message to indicate that the receipt was printed for the customer.

[0100] Having received cash and a receipt, the customer is then prompted by a display screen generated from an HTML document from the home server 90, to indicate whether they wish to conduct another transaction. The visual page or screen prompting the customer in this regard is displayed on the touch screen 30. For purposes of this example it will be assumed that the customer does not want another transaction and a message to that effect is returned through the HTML document handling portion back to the home server 90.

[0101] As shown schematically in Figure 17 in response to receiving a message that the customer is done, the home server 90 is operative to send a "go home" message to the ATM. This message preferably includes an HTML document which produces a screen display thanking the customer. This message also preferably includes embedded JAVA script which calls the JAVA applet which eventually returns the HTML document handling portion of the ATM back into connection with the URL address on the home server 90 or other address which provides the documents that are used to output the messages for the so called "attract mode". It should be remembered that the script in some embodiments may operate to cause a message to be sent from the document handling portion to an address on the home server which causes a corresponding HTTP record including the instructions comprising the desired applet to load.

[0102] As schematically indicated in Figure 18, the "go home" command applet is operative to configure the browser 76. After the HTML document handling portion is configured by the JAVA applet to return home, the JAVA applet may be configured to deliver to home server 90 information from the transaction record 104 concerning the transaction that was just completed. Because the exemplary transaction was with a customer of the institution that operates the computer system 14, all the data concerning that transaction should already be recorded in the back office 94. However it will be appreciated that this will not be the case if the transaction was conducted in response to messages from a server operated by a different institution. Thus, all or a portion of the information from the transaction record 104 may be delivered in response to a "go home" command to the home server 90 and through the CGI to the back office system 94 where it can be identified as duplicate information and discarded. This may be done using remote method invocation (RMI) to pass or deliver the object to server 90 and then transmitting the data through messages from the server to the back office or through messages or oth-

er techniques.

[0103] Of course in other embodiments transaction information may be stored in a database for extended periods rather than being returned after each transaction. Alternatively the ATM 12 may include applets which are operable to deliver transaction record information to addresses other than that of the home server, if that is desired by the operator of system 14.

[0104] The operation of the computer system when a "foreign" user uses the ATM 12 is graphically represented with regard to Figures 19 through 24. A transaction with a foreign user who is not a customer of the institution that operates ATM 12 and computer system 14, will be operated under the control of the home server 90 and will proceed in the manner of the prior example through the point where the customer inputs their card. The customer inputs a card having indicia corresponding to a URL address that does not correspond to the home server 90. The HTML document handling portion is operative to configure a message addressed to access a URL address that corresponds to the indicia on the customer's card or other address responsive to such indicia. This message is delivered to the proxy server 88 which in turn passes the message to the wide area network 18. From the wide area network the message proceeds to the foreign server corresponding to the customer's URL address. For purposes of this example the foreign server corresponds to server 96 which is connected to the Internet.

[0105] In the preferred embodiment of the invention proxy server 88 includes screening software graphically indicated 107. Screening software is preferably operable to check addresses to which messages are being directed by the ATM and to selectively prevent the sending of messages to particular addresses. This serves as a "fire wall" and is desirable for purposes of preventing fraud in the system.

[0106] As shown in Figure 20, the foreign server 96 is preferably operable to communicate HTTP messages, including HTML documents, to the ATM 12 back through the wide area network 18. This may be done using a secure socket connection ("SSC") so as to minimize the risk of interception of the messages. Of course other techniques, including encryption message techniques may be used to minimize the risk of interception of the messages.

[0107] As schematically represented in Figure 20 the response document from foreign server 96 preferably includes embedded JAVA script is representative of or corresponds to a digital signature which identifies the foreign server 96. This may be accomplished by loading an HTTP record including a signed applet, as previously discussed. An applet in application portion 84 in the ATM preferably operates to verify the digital signature in the manner described in the prior example, and sends a message indicating that the transaction has been authorized. The digital identity of the foreign institution will be stored in memory in the ATM and eventually recorded

in the back office 94.

[0108] It should be noted that the HTML documents from the foreign server 96 produce the visual pages or screens of the foreign institution which the foreign customer is accustomed to seeing. These pages may correspond to the foreign user's "home page" which are tailored specifically to the needs of the particular user.

[0109] Figure 21 shows an example of a document accessed through the foreign server 96 to the ATM 12. The document from the foreign server may include embedded JAVA script which enables operation of the JAVA applets in the manner previously discussed to operate the devices 36 in the ATM. As shown in Figure 21 the TCP/IP messages to the devices from the JAVA applets pass from the device application portion 84 to the device server 92, and the instructions therefrom to the device interfacing software portion 64 in the ATM. Device operation messages take a reverse path. As these messages pass through the device server 92, monitor software 102 monitors them to minimize the risk of fraud or abuse.

[0110] As indicated in Figure 21, the documents from the foreign server 96 may be operative to display at the touch screen 30 a request for the customer to input their PIN. The embedded JAVA script instructions would, as in the sample transaction previously discussed, include instructions that enable the keyboard 40 to accept the customer's PIN. As in the prior example, a transaction record 104 which includes a shared data object concerning this transaction would be opened by the device application software portion. As previously discussed, provisions may be made to prevent the passage of PIN data through the browser if desired.

[0111] Figure 22 indicates the return of the device operation message and PIN data to the JAVA applet, which in turn transmits the data back to the foreign server 96 through the wide area network 18 using the secure socket connection. From this point the transaction proceeds generally as previously described, except that the foreign server 96 sends the HTTP records, including HTML documents, and receives the messages from the document handling portion of the ATM. The foreign server 96 includes the JAVA application software necessary to include the embedded JAVA script in the documents that are sent to the ATM to operate the devices 36 in the machine.

[0112] As the foreign server 96 operates the machine, the monitor software 102 in the device server 92 is operative to monitor the messages in the manner previously discussed. Such monitoring would for example, operate to prevent the dispense of unduly large amounts of currency out of the machine. The monitoring software may also operate to restrict certain foreign institutions to a subset of the transaction machine devices or capabilities. This is done based on data stored in memory which limits the devices or activities that can be carried out from documents at certain addresses. This may be achieved for example through the use of code plug-ins

which implement a class of the transaction objects which limits the operations that can be performed. For example, the operations which enable connection to the foreign server may instantiate the objects which provide specified limited capabilities for messages received from the foreign server. This may for example limit the amount of money dispensed, prevent operation of a check acceptance device, limit the dispense to printed documents such as tickets, prevent operation of the cash dispenser or limit use of the machine in other appropriate ways. This may be done based on the addresses or portions of addresses for documents.

[0113] If the capabilities of the machine to the foreign customer are limited, the foreign customer may be provided with a visual interface from the foreign bank based on the transactions the machine can perform and that the owner of the machine will allow. As a result the documents accessed at the foreign bank server may be a variation of what the customer would be provided at a machine operated by the foreign bank. This could be based on documents specifically developed for operating foreign machines, or could be a variant of the usual foreign bank interface with visual indications that certain transactions are not available. In some instances the interface may indicate that some transactions are available with an associated service charge.

[0114] The ATM of the described embodiment may enhance security by limiting the addresses that the browser may access. This may be done by maintaining a list in the memory of the machine. This list may be maintained in HTTP record(s) (including documents) accessible through the home bank's intranet. The machine may access the record periodically and update the memory data. This record may itself require a digital signature corresponding to a signature in the terminal memory before the data will be loaded into terminal memory. This information may also include the instructions and information for the ATM to verify that the messages it receives by accessing documents on the foreign server are genuine. This may include digital signatures which when transferred using public key or private key encryption techniques verify the messages as genuine. The machine checks to be sure the signature in the records accessed from the foreign server corresponds to the digital signature for that address stored in memory, and enables operation of transaction devices, such as the cash dispenser, only when such correspondence is present. Of course various approaches to verifying and encrypting messages may be used in various embodiments. As used herein signatures or signed record encompass any indicia which is included in or is derivable from a record which is indicative that it is authorized.

[0115] As can also be appreciated from the foregoing disclosure, the foreign server 96 may communicate to the user through the touch screen in a language that is different from that normally used by the customers of the institution that operates the computer system 14. As

a result the HTML documents may display requests to dispense currency of a type or in an amount which is not included in the ATM. To accommodate this situation an applet is preferably included in the device application portion 84 to deal with requests for foreign currency. The foreign currency applet causes the ATM to send a message back to its home server for purposes of calculating a closest amount which may be provided to the customer in the available currency in the ATM which corresponds to what the customer requested. As will be appreciated, this applet will be operative to call the particular function address within the home server 90 that is capable of providing this function. When the dispense is made the applet is also operative to indicate to server 96 that the amount dispensed differs somewhat from the amount the customer requested. Of course in other embodiments, other approaches may be used. Alternatively an applet in the machine may generate visual displays that show equivalents in local currency when foreign currency amounts are displayed or processed. This may include presenting both amounts on visual displays presented to a user.

[0116] As represented in Figure 23, when the foreign customer has completed their transactions as indicated through the touch screen 30, the foreign server 96 is operative to send the "go home" message back to the ATM. The receipt of this message is operative in the manner previously described to cause the device application portion 84 to operate responsive to the embedded JAVA script instructions to configure the HTML document handling portion to cause the browser 76 to re-establish communication with the home server 90, or other designated document address.

[0117] As indicated in Figure 24 the applet in the device application portion 84 which processes the "go home" message is preferably operative to reconnect to the home server 90 as well as to send the transaction record information in record 104. This transaction record information which is preferably packaged in a data object, includes the customer name, the foreign institution name, digital identifier, amount information concerning amounts dispensed, transferred or deposited, and all other pertinent transaction data. The transaction data is used by applets in performing transaction steps in which any portion of the data is required. At the completion of the customer's activity at the machine an applet provides a transaction data message which includes at least a portion of the collected data. This data is communicated from server 90 through the CGI 106 to the home bank's back office 94. This information is stored in the back office for later use for purposes of settlement with the foreign bank operating the foreign server 96. Alternatively or in addition, transaction data may be recorded in the terminal in memory as well as in hard copy on a journal printer. Transaction data may be stored for downloading in a batch or by passing objects including data from many transactions. Batch data may be communicated at times and to addresses as may be stored

in memory in the terminal configuration data.

[0118] An advantage of some embodiments of the invention is that transaction data may be delivered to addresses in a local area network or in a wide area network such as the Internet. This facilitates conducting wide varieties of transactions and enables directing messages related to tracking use (such as for electronic purse type smart cards) or for settlement of various transaction types to a selected system address.

[0119] It will be appreciated that the described embodiment of the automated banking machine and system can provide an advantage that when the machine is connected to a wide area network such as the Internet, customers are able to carry out their banking transactions virtually anywhere in the world. Further, despite the broad capabilities of the system, because the machine may be monitored locally, both in terms of connection and activity, the risk of fraud is minimized.

[0120] Embodiments of the invention may include a further feature to facilitate access to documents in the network to which the machine is connected. This feature is operative to determine if an HTTP record such as an HTML document or other item is accessible at an address for downloading before the computer will attempt to access the record. This avoids transaction time outs that might otherwise occur as a result of inability to access a record due to the server through which the record is normally accessed being down. Other embodiments may consider both the size of the record and the transfer rate and determine that a transfer speed for the record is not sufficiently rapid, so that an alternative record should be transferred.

[0121] In one embodiment this feature is achieved through use of a separate program or applet which checks to see if a server that the computer will subsequently want to access is alive. The applet operates responsive to receiving an address or portion thereof, to which a connection will be made. The applet operates to make a socket connection to the address and loads a small but sufficient amount of the record or otherwise operates to determine that the server through which the record must be accessed is alive. In response to the applet verifying the operation of the remote server, or otherwise determining that conditions indicative that the record may be accessed or loaded, the computer then operates so that the browser or similar software component is enabled to navigate to the address at the appropriate time in the transaction sequence. If the applet is unable to detect that the remote server is alive, or determines that it does not appear the record may be successfully accessed or loaded, steps may be taken to access alternative addresses or to discontinue the transaction. Alternative addresses to access may be based on data stored in the memory of the terminal or may be obtained by accessing documents either locally or remotely which include data from which alternative addresses may be obtained or derived. Alternative addresses are similarly checked to make a determination

that the records can be accessed before attempts are made to access the alternative records. This approach avoids delays in carrying out transactions.

[0122] Alternative embodiments may employ other approaches to determine if desired HTTP records such as HTML documents may be successfully accessed and/or downloaded adequately before the browser providing the customer interface attempts to access the document. Such embodiments may consider in determining whether the document can be successfully accessed, the transfer speed or other conditions related to system operation or document content. For example, the applet which tests to determine that the HTTP record can be accessed, or a further applet, may determine the transfer rate at which the record can be transferred to the computer. The rate at which the data can be transferred may be compared to data stored in memory, and if the rate is slower than the data representative of the desired stored rate an alternative record is accessed. This may be for example an HTML document stored locally in the machine. Other embodiments may include programs which consider the size of the HTTP record and the transfer rate in determining a transfer speed. Such programs then determine if the record can be transferred fast enough to suit the parameters established in the configuration in memory, and if not, alternative addresses are accessed. Such alternative records may be similarly tested for transfer speed before being transferred.

[0123] Programs may also consider other factors in deciding to access a particular address, such factors may include for example day and time information, or information from sensors such as sensors in a floor indicating that other persons are waiting to use the machine. In this way access to documents that have extensive outputs which may tend to prolong transactions can be avoided even when records can be loaded at an adequate speed.

[0124] While the described embodiment of the automated banking machine and system of the present invention is shown with regard to a particular type of machine that is made specifically for connectivity to local or wide area networks, conventional automated banking machines may also be adapted to include such capability. Specifically the HTML document handling portion and device application portions may be included with other conventional software which operates within an automated banking machine. This enables such ATMs to operate either in the conventional proprietary network or as part of a wide area network. In addition, automated banking machines may be configured to operate their devices through the device interfacing software portion described herein or through a different software interface when operating in a conventional network. Such machines may switch to requiring device messages to be passed through a device server when operating under the control of a server within the wide area network to maintain security within the system. In this way a sin-

gle ATM could operate in proprietary networks in the manner of current ATMs as well as in the network configuration of the system described herein.

[0125] Alternative embodiments of the invention operate to communicate transaction messages used in a proprietary ATM network. This may be accomplished by using a CGI in connection with either the HTML document handling portion of the ATM or the HTTP home server or other server. The CGI operates in connection with a message conversion program and database to cull the necessary data from the HTML documents and response messages and generate the defined transaction request messages appropriate for the proprietary transaction network. Likewise, the message conversion program and CGI operate to receive function command messages from the proprietary network and convert them and generate appropriate HTML documents and/or TCP/IP messages for use by the ATM. Because these proprietary network formats are defined and the data necessary to produce and interpret the messages are known, the use of the ATM 12 directly in a conventional proprietary ATM network is achieved.

[0126] Conventional ATM transaction messages are defined layout messages that do not include HTML documents on HTTP messages. An example of known conventional messages used to operate ATMs are Diebold 91X messages. Such messages generally involve transmission of a request message from an ATM in a defined layout including customer input data (account/pin) and an indication of the type and amount of transaction requested. The request message is received by an ATM host computer which sends back a response message with a defined layout which includes an indication whether the transaction is authorized. The ATM then returns another message to the host computer indicating whether the machine was able to carry out the transaction. The messages used in such conventional proprietary networks generally occupy relatively little band width.

[0127] In connecting an ATM according to an embodiment of the invention to such a network, a server is provided. The server is in operative connection with a memory which includes a relational database which holds the message conversion and document creation data. In one configuration, the server is connected to the document handling portion through a network, or may reside on the computer of the ATM. The server produces the documents which the browser accesses and which include the transaction device instructions. The server (or a connected server) communicates the conventional messages with the host. One server may provide an interface for several ATMs connected to it in a LAN, or alternatively, each ATM may have its own server operating therein.

[0128] The ability of ATM 12 to communicate in a proprietary network also enables operation of the ATM in a manner in which the interface is generated by a user's home institution in the manner previously described, but

in which transactions are authorized through messages directed through a proprietary ATM network. This achieves the security of using the proprietary network while providing the customer with the advantages of the familiar home bank interface and/or "personal home page" interface.

[0129] In such a configuration the ATM transaction function devices may be operated in a conventional manner in response to conventional ATM transaction messages such as Diebold 91X messages. In the proprietary network. The customer output devices, such as the screen (and speakers if provided) communicate through a browser connected to a local or wide area network. The browser accesses documents to prompt a customer through operation of a transaction, but the documents do not include instructions which cause operation of devices such as the cash dispenser.

[0130] In one configuration the browser may be operated by the computer in response to the status of devices in the machine, as the devices are operated in response to conventional ATM messages. In this manner the browser may be navigated to selected addresses, including addresses which are associated with the customer based on customer input data. However, as the documents received by the browser will not operate the transaction function devices, there is less need for security measures in accessing documents. As a result, the customer may still operate the machine in response to a familiar and unique interface, and marketing information such as advertising or other material may be presented in the transaction sequence.

[0131] In other embodiments machines may perform some device functions based on conventional messages, while others may be performed in response to instructions in HTML documents or other HTTP messages. For example HTML documents may provide considerable data for use by printers or other output devices. Some embodiments may access documents with instructions, but may ignore some and act in response to others. The approach may be selected by the systems operator by configuring the software based on their requirements.

[0132] A further advantage of the system configuration of one preferred embodiment is that it has enhanced flexibility for communicating messages associated with the ATM. The device manager 68 preferably generates status messages associated with the status of devices 36. These status messages may commonly represent information about conditions which exist at the devices. Such messages may indicate that supplies of paper for printers or currency, are low or are depleted. Other messages may indicate that devices are not functioning properly. Often such messages indicate that the ATM requires servicing. All such types of messages are referred to herein interchangeably as status or fault messages.

[0133] The device interfacing software portion 64 communicates through the intranet 16 using TCP/IP

messages. While the messages associated with transactions previously described are directed to the device server 92, the software portion 64 may include a server and be configured to address fault and status messages to other addresses in the intranet or the Internet. For example, such fault or status messages may be directed to a software application which delivers messages to a service provider. Further, fault messages may be selectively directed based on the nature of the fault indicated. For example, fault messages indicative of a need to replenish currency or supplies may be directed to an address in the intranet associated with an entity who has responsibility for replenishing supplies. Alternatively, fault messages which indicate a need for other types of servicing may be directed to an address associated with an entity who can provide the type of servicing required.

[0134] Alternatively, the selective dispatching of fault messages to addresses in the intranet 16 may be accomplished by appropriately configuring device server 92. In addition, either software portion 64 or device server 92 may direct fault messages from the ATMs to a fault handling system such as to a computer operating Event Management System™ software available from Diebold, Incorporated. Such software is operative to resolve the nature of the fault condition and to notify appropriate personnel of the corrective action to be taken.

[0135] The ATM 12 may further include a software function to assist in diagnosing problems and providing remedial service. As graphically represented in Figure 2, alternative embodiments of the ATM 12 may include a mini-HTTP server 109 which is in communication with the device interfacing software portion 64. Server 109 is configured to receive device status messages and to produce HTTP records including HTML documents in response thereto, which provide data representative of device status to a diagnostic device 110 such as a hand held computer terminal. Server 109 includes a CGI for interfacing with the device software so that a technician may access the information in the records accessible at the HTTP addresses related to status messages and input test and corrective instructions through diagnostic device 110. The HTTP records and/or HTML documents generated by server 109 may preferably include graphic and audio instructions indicative of conditions such as problems, as well as corrective action data and repair instructions.

[0136] In alternative versions of the invention the functions of the mini-HTTP server 109 may reside in device server 92. This may be particularly appropriate where the function of the device server resides on the computer in the ATM. Regardless of where the function resides the use of the visual and audio components of HTML documents associated with maintenance and diagnostic messages facilitates servicing of the ATM.

[0137] These records delivered through the mini-HTTP server include instructions that correspond to the status or fault conditions. Such records or documents may be accessed locally as previously discussed, or re-

motely. A technician using a hand held computer which includes a browser or other software operative to access the HTTP records may access the documents locally for purposes of maintenance, diagnosis and servicing. In some situations the customer interface and browser associated therewith may be used to access the mini-HTTP server, or a separate browser, display and input devices on the machine and intended for use servicing activity may be used. Alternatively, the fault and status messages may be monitored from terminals at locations anywhere that are connected in the network. The mini-HTTP server handling status and fault messages may also be configured to send an email or similar message to a selected address whenever a particular condition or group of conditions exist.

[0138] A further advantage of this feature is that HTTP messages may also be sent to the mini-HTTP server to attempt to correct problems. Such messages may include running diagnostic tests and receiving results. It may also include operating devices to test or attempt to clear jams and other malfunctions. This can often be done from remote locations. Of course, when there is a significant risk of unauthorized access to the server handling default or device messages, appropriate security measures should be taken.

[0139] The HTTP records which indicate the status of the transaction function devices may have different forms depending on the software configuration and the needs of the system operator. In some embodiments the device status information for one or more devices may be represented by indicia contained within a data object. The data object may be transferred to other connected computers to provide the status data. The transfer of the data object may be accomplished by remote method invocation (RMI) for example. The data in the transferred data object may then be used to generate message and/or outputs desired by the system operator. This technique may be particularly useful when the operator wishes to connect the machine to an existing monitoring system and indicia included in the data object can be used to generate outputs or messages indicative of device status that can be processed by the existing system. Plug-ins may further be used to achieve communication between existing monitoring systems and transaction machines which have different types of status conditions or different types of message formats. This includes machines which have different types of transaction function devices and capabilities.

[0140] The technique of transferring a data object may also be used to conduct testing or modification of transaction function devices. For example, indicia in the data object may be modified by a servicer and the object passed back to the machine. The software in the machine may cause the transaction function devices to operate or change conditions or programming in response to the modified data object. This may include for example clearing a fault indication or causing a device to operate to clear a jam or to conduct a test. The results of

such activity may be reflected in modified indicia in the data object which may then be transferred to the computer in the diagnostic terminal. Of course, the approaches discussed herein are exemplary and other approaches will become apparent to those skilled in the art from the description herein.

[0141] Figure 25 shows a schematic view of a network configuration for an alternative embodiment of the automated banking machine.

[0142] The embodiment shown in Figure 25 includes an automated banking machine specifically adapted for operating in connection with conventional automated banking machine systems such as systems which operate using Diebold 91X ATM message formats or other non-HTTP conventional format. A host computer 120 is a conventional ATM host which communicates using such messages. The host communicates with an interface server schematically indicated 122. Interface server 122 operates in the manner previously discussed and is in operative connection with a memory that includes the information necessary to convert HTTP messages that pertain to a transaction request to a 91X request message or other conventional message, which can be handled by host computer 120. Likewise interface server 122 and the instructions and data stored in memory are operative to convert a conventional 91X command message or other conventional command message from the host 120 into HTTP messages which can be used by the automated banking machine to carry out the command. Similarly interface server 122 is operative to receive the HTTP messages which correspond to the response of the automated banking machine to the commands and to produce a 91X response message or other conventional response message to the host. In accomplishing these functions the interface server communicates with a interface client 124 which in the preferred embodiment is a COMM plug in which operates on the banking machine terminal under a Windows NT® operating environment. Interface server 122 also includes a command/status gateway 126. The command/status gateway is operative to receive command and status messages from the software portions handling the functional devices within the machine. The messages concerning the devices are used in producing transaction messages to send back to host 120. In addition, the command status gateway portion also produces status messages indicative of the status of devices which may also be communicated to the host.

[0143] The interface server 122, command status gateway portion 126 and interface client 124 may reside in software on the automated banking machine terminal. In this configuration the terminal appears to the host computer to be a conventional machine. Alternatively interface server 122 and command status gateway portion 126 may reside on a separate server, while the interface client portion 124 may reside on the terminal. This enables the interface server 122 to handle a number of automated banking machines by connecting

the machines to the interface server through a network.

[0144] The alternative configuration of the automated banking machine system shown in Figure 25 is particularly adapted for use in connection with existing ATM system. The machine includes an HTML document handling portion 128 which includes a browser which operates in the manner of the embodiments previously described. The HTML document handling portion is alternatively referred to as a browser herein for purposes of simplicity. The HTML document handling portion operates in connection with a network 130 to access HTTP records in the form of HTML documents through servers 132, 134 and 136. For purposes of this example server 132 will be considered the server of the home bank which operates the automated banking machine. The browser portion 128 is enabled to access documents of its home bank for purposes of obtaining content and instructions for purposes of outputting information to customers as well as for operating devices on the machine. Servers 134 and 136 are representative of other servers which the automated banking machine may be instructed to access for purposes of downloading documents which include information or instructions. Often such documents from non-home bank servers will include information which is to be presented to customers such as advertising, promotional material, stock quotations or other types of information. It should be understood that the servers 134 and 136 may be directly connected to network 130 or may be accessed through other networks and servers. In some embodiments such servers may be accessed through the internet for purposes of providing documents to the automated banking machine.

[0145] Document handling portion 128 includes a terminal theater software portion schematically indicated 138. Terminal theater portion 138 is schematically shown in greater detail in Figure 26. Terminal theater portion 138 includes a back stage frame 140 and a theater frame 142. The back stage frame 140 although it resides in the browser, is not visible on the screen of the automated banking machine. The theater frame 142 is a visible frame and controls what is shown to the customer.

[0146] As schematically represented in Figure 25 the HTML document handling portion also includes a terminal director portion 144. The terminal director portion includes directors which are related instances of applets which are used in carrying out particular types of transactions. The terminal directors generally correspond to the operation of the JAVA applets in the previously described embodiment.

[0147] The automated banking machine of the alternative embodiment further includes a transaction services application (TSA) schematically indicated 146. The transaction services application provides security, terminal condition, terminal authorization and key management services within the automated banking machine. The transaction services application includes a function